UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,756	12/24/2003	Steven N. Simon	P3136-938	8932

62665   7590   12/10/2009
BUCHANAN INGERSOLL & ROONEY, PC
P.O. BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
LI, GUANG W

ART UNIT	PAPER NUMBER
2446	

NOTIFICATION DATE	DELIVERY MODE
12/10/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

	Application No.	Applicant(s)
	10/743,756	SIMON ET AL.
Office Action Summary	Examiner	Art Unit	
	GUANG LI	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _17 August 2009_.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1,12,14,16,17,27,28,39,41,43,44,47,48 and 51-64_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1,12,14,16,17,27,28,39,41,43,44,47,48 and 51-64_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _01 June 2004_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All   b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   It is hereby acknowledged that the following papers have been received and placed of record in the file: Amendment date 08/17/2009

2.   Claims 1, 12, 14, 16-17, 27-28, 39, 41, 43-44, 47-48, and 51-64 are presented for examination.

Response to Arguments

3.   Applicant's arguments with respect to claims 1, 12, 14, 16-17, 27-28, 39, 41, 43-44, 47-48, and 51-64 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4.   Claims 52 is rejected under 35 U.S.C. 102(b) as being anticipated by Peacock (US 6,381,650).

5.   Regarding claim 52, Peacock teaches a method for a client computer to find a network address of a server computer, the method comprising:

performing a primary search procedure, the primary search procedure including searching a local storage of the client computer system for the network address of the server computer (search for previously IP address of the server not available "the client program 137 first determines if it has a previously known IP address of the server program 117 at step 305. If a previous IP address is not available, then client program proceeds to step 350 in order to perform a normal domain name service look-up" see Peacock: col.4 lines 48-56; Fig 3a-3b elements 305 350 and 380);

performing a backup search procedure if the network address of the server computer is not found using a primary search procedure (DNS domain name service lookup if the address of previously IP address of the server not available "the client program 137 first determines if it has a previously known IP address of the server program 117 at step 305. If a previous IP address is not available, then client program proceeds to step 350 in order to perform a normal domain name service look-up" see Peacock: col.4 lines 48-56; Fig 3a-3b elements 305 350 and 380), the backup search procedure including searching a configuration record of the client computer system for the network address of the server computer (desired server address in forwarding address file when addresses has moved "If the hostname from the "Are you there?" packet matches a hostname in the forwarding address file, then the server program prepares a "addressee has moved" packet at step 690. The "addressee has moved" packet contains the hostname of the desired server and the associated forwarding IP address of the desired server" see col.7 lines 50-58); and

establishing a connection with the server computer using the network address found (establish connection when server IP address determined "Thus, if a response packet is received the client program proceeds to step 380 and begins to access the server" see Peacock: col.6 lines 16-18; Fig. 3b item 380).

Claim Rejections - 35 USC § 103

6.   The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7.   Claims 1, 12, 17, 28, 39, 44, 48, 53-54, 58-64 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Peacock (US 6,381,650) in view of Pitsos (US 2006/0168445 A1).

8.   Regarding claim 1, Peacock teaches a method for a client computer to find a network

address of a password server computer having a public key, the method comprising:

        searching for a network address of the server computer using a backup search procedure

if the address of the server computer cannot be identified using a primary search procedure (DNS

domain name service lookup if the address of previously IP address of the server not available

"the client program 137 first determines if it has a previously known IP address of the server

program 117 at step 305. If a previous IP address is not available, then client program proceeds

to step 350 in order to perform a normal domain name service look-up" see Peacock: col.4 lines

48-56; Fig 3a-3b elements 305 350 and 380); and

        establishing a connection with the server computer using the network address found

(establish connection when server IP address determined "Thus, if a response packet is received

the client program proceeds to step 380 and begins to access the server" see Peacock: col.6 lines

16-18; Fig. 3b item 380),

        wherein:

        the backup search procedure searches for the server computer to identify the server

computer (DNS backup search "If no response is received after subnet scanning, then the client

program proceeds to step 350 to perform standard method of obtaining a server address: domain

name service (DNS). At step 350, the client program attempts to resolve the hostname of the

desired server with a domain name server" see Peacock: col.6 lines 19-28).

Peacock does not explicitly discloses the public key is an identifier of the server computer, and using the public key to identify the server computer.

However Pitsos teaches the public key is an identifier of the server computer, and using the public key to identify the server computer (public key information of the server address "the gateway 12 determines an internal network address of the internal device 13 based on the public key information included in the incoming data as well as the stored list of public key identifiers and associated internal network addresses" see Pitsos: ¶[0033]; ¶[0035]) in order to provide selectively in accordance with the entity requesting the information for security purpose.

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Peacock to include (or to use, etc.) the public key is an identifier of the server computer, and using the public key to identify the server computer as taught by Pitsos in order to provide selectively in accordance with the entity requesting the information for security purpose.

9.   Regarding claim 12, the modified Peacock taught a method of to claim 1 as described above. Pitsos further comprising the step of authenticating the server computer after the connection has been established (authentication processes "The cryptographic unit 26 performs any required encryption, decryption, signature, signature verification or authentication processes" see Pitsos: ¶[0043]).

10.   Regarding claim 17, claim 17 is rejected for the same reason as claim 1 set forth hereinabove. Regarding claim 17, the modified Peacock taught the claimed method, therefore together, they teach the claimed system.

11.   Regarding claim 28, claim 28 is rejected for the same reasons as claim 1 set forth

hereinabove. Regarding claim 28, the modified Peacock the claimed method, therefore together,

he teaches the claimed computer readable data storage device.

12.   Regarding claim 39, claim 39 is rejected for the same reason as claim 12 as set forth

hereinabove.

13.   Regarding claim 44, Peacock teaches a method for a client computer to locate a network

address of a server computer on a computer network, said server computer having a public key

that is an identifier of the server computer, the method comprising:

        searching for the address of the server computer in a local system storage of the client

computer (DNS domain name service lookup if the address of previously IP address of the server

not available "the client program 137 first determines if it has a previously known IP address of

the server program 117 at step 305. If a previous IP address is not available, then client program

proceeds to step 350 in order to perform a normal domain name service look-up" see Peacock:

col.4 lines 48-56; Fig 3a-3b elements 305 350 and 380); and

        performing a backup search procedure if the address is not found in the local system

storage (DNS backup search "If no response is received after subnet scanning, then the client

program proceeds to step 350 to perform standard method of obtaining a server address: domain

name service (DNS). At step 350, the client program attempts to resolve the hostname of the

desired server with a domain name server" see Peacock: col.6 lines 19-28), the backup search

procedure being selected **from a group** of search procedures including the following:

        broadcasting a message over the network to identify the address of the server computer

(direct broadcast messages allocate server address "the bits of the subnet mask 510 of the desired

server are inverted to generate an inverted subnet mask 520. The inverted subnet mask 520 will

have zeros ("0") in the Network/Subnet portion and ones ("1") in the host portion" see col.5 lines

39-65),

       searching an authentication record for the address of the server computer,

       using a loop back address,

       using a inter process communication to determine whether the server computer is running

on a same CPU as the client computer in order to determine the network address, and

       searching a configuration record of the client computer for the address of the server

computer (desired server address in forwarding address file when addresses has moved "If the

hostname from the "Are you there?" packet matches a hostname in the forwarding address file,

then the server program prepares a "addressee has moved" packet at step 690. The "addressee has

moved" packet contains the hostname of the desired server and the associated forwarding IP

address of the desired server" see col.7 lines 50-58); and

       establishing a connection with the server computer using the network address found

(establish connection when server IP address determined "Thus, if a response packet is received

the client program proceeds to step 380 and begins to access the server" see Peacock: col.6 lines

16-18; Fig. 3b item 380).

       Peacock does not explicitly discloses the public key is an identifier of the server

computer, and using the public key to identify the server computer.

       However Pitsos teaches the public key is an identifier of the server computer, and using

the public key to identify the server computer (public key information of the server address "the

gateway 12 determines an internal network address of the internal device 13 based on the public

key information included in the incoming data as well as the stored list of public key identifiers and associated internal network addresses" see Pitsos: ¶[0033]; ¶[0035]) in order to provide selectively in accordance with the entity requesting the information for security purpose.

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Peacock to include (or to use, etc.) the public key is an identifier of the server computer, and using the public key to identify the server computer as taught by Pitsos in order to provide selectively in accordance with the entity requesting the information for security purpose.

14.   Regarding claim 48, claim 48 is rejected for the same reason as claim 44 as set forth hereinabove. Regarding claim 44, the modified Peacock taught the claimed method, therefore together, they teach the claimed system.

15.   Regarding claim 53, Peacock taught the method for a client computer to find a network address of a server computer as described hereinabove. Peacock does not explicitly discloses the server computer is a password server computer having a public key that is an identifier of the server computer, and the primary search procedures or the backup search procedures searches for the server computer using the public key to identify the server computer.

However Pitsos teaches the server computer is a password server computer having a public key that is an identifier of the server computer, and the primary search procedures or the backup search procedures searches for the server computer using the public key to identify the server computer (public key server and public key information of the server address "the gateway 12 determines an internal network address of the internal device 13 based on the public key information included in the incoming data as well as the stored list of public key identifiers

and associated internal network addresses" see ¶[0033]; ¶[0035]) in order to provide selectively

in accordance with the entity requesting the information for security purpose.

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Peacock to include (or to use, etc.) the server computer is a password

server computer having a public key that is an identifier of the server computer, and the primary

search procedures or the backup search procedures searches for the server computer using the

public key to identify the server computer as taught by Pitsos in order to provide selectively in

accordance with the entity requesting the information for security purpose.

16.   Regarding claim 54, Peacock teaches a method for a client computer to find a network

address of a server computer, the method comprising:

performing a primary search procedure (search for previously IP address of the server not

available "the client program 137 first determines if it has a previously known IP address of the

server program 117 at step 305. If a previous IP address is not available, then client program

proceeds to step 350 in order to perform a normal domain name service look-up" see Peacock:

col.4 lines 48-56; Fig 3a-3b elements 305 350 and 380);

performing a backup search procedure if the network address of the server computer is

not found using a primary search procedure (DNS domain name service lookup if the address of

previously IP address of the server not available "the client program 137 first determines if it

has a previously known IP address of the server program 117 at step 305. If a previous IP

address is not available, then client program proceeds to step 350 in order to perform a normal

domain name service look-up" see Peacock: col.4 lines 48-56; Fig 3a-3b elements 305 350 and

380), and

establishing a connection with the server computer using the network address found (establish connection when server IP address determined "Thus, if a response packet is received the client program proceeds to step 380 and begins to access the server" see Peacock: col.6 lines 16-18; Fig. 3b item 380).

Peacock does not explicitly disclose backup search procedure searching an authentication record for the network address of the server computer.

However Pitsos teaches the backup search procedure searching an authentication record for the network address of the server computer (authentication processes "The cryptographic unit 26 performs any required encryption, decryption, signature, signature verification or authentication processes" see Pitsos: ¶[0043]) in order to provide security purpose.

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Peacock to include (or to use, etc.) the backup search procedure searching an authentication record for the network address of the server computer as taught by Pitsos in order to provide security purpose.

17.   Regarding claim 58, the modified peacock taught the method of claim 1 as described hereinabove. Peacock further teaches wherein the public key identifies a plurality of server computers having different network addresses (different IP address from the previous IP address "If the current IP address is from a different network or subnet than the previous IP address, then the server program sends a directed broadcast "forwarding address" packet to the subnet of the previous IP address at step 620" see Peacock: col. 6 lines 63 – col.7 lines 1-6).

18.   Regarding claim 59, claim 59 is rejected for the same reason as claim 58 as set forth hereinabove.

19.   Regarding claim 60, claim 60 is rejected for the same reason as claim 58 as set forth

hereinabove.

20.   Regarding claim 61, claim 61 is rejected for the same reason as claim 58 as set forth

hereinabove.

21.   Regarding claim 62, the modified peacock taught the system of claim 48 as described

hereinabove. Peacock further teaches wherein the server means includes a pluatlity of server

computers having the same public key and different network addresses (different IP address from

the previous IP address "If the current IP address is from a different network or subnet than the

previous IP address, then the server program sends a directed broadcast "forwarding address"

packet to the subnet of the previous IP address at step 620" see Peacock: col. 6 lines 63 – col.7

lines 1-6).

22.   Regarding claim 63, claim 63 is rejected for the same reason as claim 58 as set forth

hereinabove.

23.   Regarding claim 64, claim 64 is rejected for the same reason as claim 62 as set forth

hereinabove.

24.   Claims 14, 16, 27, 41, 43, 47 and 51 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Peacock (US 6,381,650) in view of Pitsos (US 2006/0168445 A1) and further

in view of Lim et al (US 6,014,660).

25.   Regarding claim 14, the modified Peacock taught a method of to claim 1 as described

above. The modified Peacock does not explicitly comprising populating a local storage of the

client computer with a list of network addresses for server computers after the connection has

been established.

However Lim teaches the comprising populating a local storage of the client computer

with a list of network addresses for server computers after the connection has been established

(list of preferred address "For example, if the record includes a symbolic name and a preferred IP

address, the client DNS process 214 translates the symbolic name to generate a list of all IP

Addresses that correspond to the symbolic name. Preferably, this translation is performed by

sending a DNS request to the DNS server system 102. After translating the symbolic name, the

client DNS process 214 tests to see if the preferred address is included in the list of addresses"

see Lim: col.8 lines 37-54) in order to provide alternated backup server address for system

failure purpose.

It would have been obvious to one of ordinary skill in the art at the time of invention to

create the invention of Peacock to include (or to use, etc.) the comprising populating a local

storage of the client computer with a list of network addresses for server computers after the

connection has been established as taught by Lim in order to provide alternated backup server

address for system failure purpose.

26.   Regarding claim 16, the modified Peacock taught a method of to claim 1 as described

above. Lim further teaches wherein the primary and backup search procedures are performed in

parallel (iterative translation perform parallel DNS lookup "When client-sensitive translation is

not required, the DNS server performs iterative or recursive DNS translation" see Lim:

Abstract).

27.   Regarding claim 27, claim 27 is rejected for the same reason as claim 16 as set forth

hereinabove.

28.   Regarding claim 41, claim 41 is rejected for the same reason as claim 14 as set forth

hereinabove.

29.   Regarding claim 43, claim 43 is rejected for the same reason as claim 16 as set forth

hereinabove.

30.   Regarding claim 47, the modified Peacock taught a method for a client computer to find a

network address of a server according to claim 44, as described above. Lim further teaches

wherein the backup search procedure is performed in parallel with searching the local system

storage of the client (searching local DNS database "In step 506 the result of this search is

examined, by the DNS server system 102, to determine if any associated records were found in

DNS database 116" see Lim: col.6 lines 57-63; Fig.1 item 116).

31.   Regarding claim 51, claim 51 is rejected for the same reason as claim 47 as set forth

hereinabove.

32.   Claims 55-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peacock

(US 6,381,650) in view of Kulkarni et al. (US 2003/0182433 A1).

33.   Regarding claim 55, Peacock teaches a method for a client computer to find a network

address of a server computer, the method comprising:

        performing a primary search procedure (search for previously IP address of the server not

available "the client program 137 first determines if it has a previously known IP address of the

server program 117 at step 305. If a previous IP address is not available, then client program

proceeds to step 350 in order to perform a normal domain name service look-up" see Peacock:
col.4 lines 48-56; Fig 3a-3b elements 305 350 and 380);

performing a backup search procedure if the network address of the server computer is
not found using a primary search procedure (DNS domain name service lookup if the address of
previously IP address of the server not available "the client program 137 first determines if it
has a previously known IP address of the server program 117 at step 305. If a previous IP
address is not available, then client program proceeds to step 350 in order to perform a normal
domain name service look-up" see Peacock: col.4 lines 48-56; Fig 3a-3b elements 305 350 and
380), and

establishing a connection with the server computer using the network address found
(establish connection when server IP address determined "Thus, if a response packet is received
the client program proceeds to step 380 and begins to access the server" see Peacock: col.6 lines
16-18; Fig. 3b item 380).

Peacock does not explicitly disclose backup search determining whether the server
computer is running on a CPU that is the same CPU on which the client computer is running in
order to determine the network address of the server computer.

Kulkarni teaches backup search determining whether the server computer is running on a
CPU that is the same CPU on which the client computer is running in order to determine the
network address of the server computer (using loopback address to determines home agent
address "The virtual Home Agent address may be implemented in a variety of ways, such as
through the use of a loopback address" see Kulkarni: ¶[0042]) in order to efficient using resource
and testing connectivity between the nodes.

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Peacock to include (or to use, etc.) the backup search determining whether the server computer is running on a CPU that is the same CPU on which the client computer is running in order to determine the network address of the server computer by Kulkarni in order to provide selectively in accordance with the entity requesting the information for security purpose.

34.   Regarding claim 56, the modified Peacock taught a method according to claim 55, as described above. Kulkarni further teaches wherein determining whether the server computer is running on the same CPU as the client computer comprises using a loop back address of the server computer (using loopback address to determines home agent address "The virtual Home Agent address may be implemented in a variety of ways, such as through the use of a loopback address" see Kulkarni: ¶[0042]).

35.   Claims 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peacock (US 6,381,650) in view of Kulkarni et al. (US 2003/0182433 A1) and in further view of Fraser (US 5,434,914).

36.   Regarding claims 57, the modified Peacock taught the a method according to claim 55 as set hereinabove. The modified Peacock do not explicitly discloses determining whether the server computer is running on a CPU of the client computer comprises sending out an inter process communication to the CPU.

Fraser teaches determining whether the server computer is running on a CPU of the client computer comprises sending out an inter process communication to the CPU (communication between the components may be by means of function invocations or inter-process

communications see Fraser: col.8 lines 35-38). Fraser further provides the advantage of a

translation of a name into a network address done in a first node of a network (see Fraser: col.3

lines 14-16).

It would have been obvious to one of ordinary skill in the art, having the teachings of the

modified Peacock before them at the time the invention was made to modify the method to find

network address of server computer of the modified Peacock to includes whether the server

computer is running on a CPU of the client computer comprises sending out an inter process

communication to the CPU as taught by Fraser.

One of ordinary skill in the art would have been motivated to make this modification in

order to provide unique way communication between the components for improve

communication system in view of Fraser.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Guang Li whose telephone number is (571) 270-1897. The

examiner can normally be reached on Monday-Friday 8:30AM-5:00PM(EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jeff Pwu can be reached on (571) 272-6798. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 8, 2009
GL
Patent Examiner

/Benjamin R Bruckart/
Primary Examiner, Art Unit 2446